AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One Apple Macintosh Tower Computer and Neaby Cellular Telephones and Digital Media, currently located at 840 SW Englewood Dr., Lake Oswego OR 97034

Case No. 3:20-mc-1329

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

One Apple Macintosh Tower Computer and Neaby Cellular Telephones and Digital Media, currently located inside 840 SW Englewood Dr., Lake Oswego OR 97034, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section (TITLE(S) & SECTION(S))	*Offense Description* (GENERAL DESCRIPTION OF OFFENSE(S))
18 USC §§ 1028A, 1343, 1957	Aggravated Identity Theft, Wire Fraud, and Money Laundering

The application is based on these facts:

See affidavits which are attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher Mar, Special Agent, IRS-CI

Printed name and title

Sworn via telephone pursuant to Fed. R. Crim. P. at 1:29 p.m .

Date: December 22, 2020

Youlee Yim You

Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CHRISTOPHER MAR

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Christopher Mar, being duly sworn, do hereby depose and state as follows:

Introduction

1. I submit this affidavit in support of an application under Rules 41 and 4.1 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure, search, and examination of the tower computer, cellular telephones, and associated digital storage media (including thumb drives, discs, SIM cards) (hereinafter "Devices"), which are currently in the living room of the residence at 840 SW Englewood Drive in Lake Oswego, Oregon, 97034, as described in Attachment A hereto, and the extraction of electronically stored information from the Devices, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, sections 1028A, 1343, and 1957.

2. This affidavit incorporates in full as though restated herein the accompanying affidavit in support of a criminal complaint against DAVID ROGER UNITAN (UNITAN), which this Court issued on December 21, 2020, at 4:15 p.m., with the exception of the whereabouts of UNITAN (who is now in federal custody) and the property for which seizure warrants were issued in this matter. It is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge

obtained from other individuals during my participation in this investigation, my own review of records related to this investigation, and information gained through my training and experience.

Statement of Probable Cause

3. On December 22, 2020, at approximately 8:00 a.m., Special Agents with IRS-CI and Deputies with Clackamas County Sheriff's Office (CCSO) went to the residence of 840 SW Englewood Drive in Lake Oswego, Oregon, to arrest UNITAN and to seize fruits of the above-listed offenses pursuant to warrants issued by this Court on December 21, 2020.

4. When UNITAN answered the door, he was not wearing shoes. After being taken into custody, he asked to be allowed to put on shoes before departing. The first pair of shoes UNITAN proposed donning had shoelaces, which are discouraged for persons entering Federal custody. Arresting officers asked UNITAN if he had a pair of shoes without laces. He responded that he had a pair of slip-on boat shoes in the living room. UNITAN led CCSO Deputy Wilson and me into the living room of the residence to retrieve those shoes.

5. In plain view in the living room with UNITAN, I observed he had dual computer monitors on a desk. The monitors were Apple Macintosh ProDisplay XDRs and apparently connected to a large Apple Macintosh tower on the floor beneath the desk. UNITAN claimed he did not have any other computers in the residence.

6. I also observed several cell phones and thumb drives on the desk and nearby couch. I know UNITAN has used multiple phone numbers in connection with the offenses described in the incorporated affidavit, and several of those phones have been associated with Telnyx, a cellular telephone service provider. I saw multiple Telnyx sim cards on the desk with the computer.

7. UNITAN's ex-wife, Janet Marie Kennedy, was called to pick up UNITAN's fourteen-year-old son, who was also at the residence. Ms. Kennedy advised us that she was unaware of any employment UNITAN maintained, but she mentioned he had told her he was investing in bitcoin. Based on the financial records I have reviewed, UNITAN does not appear to be employed or to have any legitimately obtained income.

8. Other than UNITAN's son, no other person was at the residence, and according to Ms. Kennedy, UNITAN's children rarely stay there. I observed no signs of any other inhabitants in the residence while executing the above-referenced warrants.

9. I know that the SBA EIDLs and PPP loans at issue in this investigation were applied for electronically. Based on an analysis of his bank records, I also know UNITAN opened many of the bank accounts into which the fraudulently obtained loan proceeds were deposited using the internet and that he purchased bitcoin through the exchange Cex.io.

10. Based on my training and experience, people engaging in digital financial frauds and people who maintain online bank and cryptocurrency accounts keep records of their financial transactions on their computers or other electronic device, including smartphones. Accordingly, I believe there will be evidence of fraudulent SBA loan applications, bank accounts used to receive the proceeds of those applications, assets purchased with the proceeds of those applications, and access to cryptocurrency exchanges on UNITAN's computer and cellular telephones. Additionally, I believe there is likely to be evidence of additional fraudulently opened bank accounts that this investigation has not yet revealed.

11. The Devices currently remain undisturbed at UNITAN's residence at 840 SW Englewood Drive in Lake Oswego, Oregon. Following the execution of the aforementioned

arrest and seizure warrants, law enforcement personnel remained near the premises to secure them pending the issuance of the requested warrant.

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Cellular telephone*. A cellular (or mobile or wireless) telephone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. *GPS*. A GPS navigation device uses the Global Positioning System to display its current location. It often contains historical records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated as "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock.

Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c. *Storage medium*. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, thumb drives, and other magnetic or optical media.

d. *IP address*. An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. *Internet*. The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. Based on my training and experience, I know that the Devices have capabilities that allow them to serve as Internet-connected computers, wireless telephones, digital cameras, and GPS navigation devices. In my training and experience, examining data stored on devices

of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

15. There is probable cause to believe that things that were once stored on the Device will still be stored there because, based on my knowledge, training, and experience, I know:

a. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. Data on the Device can provide evidence of a file that was once on the Device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to commit a crime, such as filing fraudulent loan applications and laundering fraud proceeds through online bank accounts over the Internet, the electronic device will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

17. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

18. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

19. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

20. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Devices to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

21. If the Devices contain evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

22. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

23. *Manner of execution*. Law enforcement personnel have secured the residence, which remains unlocked, and will enter the residence upon issuance of the requested warrant to seize the Devices.

Conclusion

24. Based on the foregoing, I have probable cause to believe, and I do believe, that the Devices described in Attachment A contain evidence**,** fruits, and instrumentalities of violations of Title 18, United States Code, sections 1028A, 1343, and 1957, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Devices described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

25. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States

Attorney Ryan W. Bounds, who informed me that, in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

CHRISTOPHER MAR
Special Agent
IRS, Criminal Investigation

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 1:29 p.m. ~~xxxxxxx~~ a.m./p.m. on December 22nd, 2020.

Youlee Yim You

HONORABLE YOULEE YIM YOU
United States Magistrate Judge